UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,178	03/30/2004	Uttam K. Sengupta	1000-0042	5846

7590 07/19/2006

The Law Offices of John C. Scott, LLC
c/o PortfolioIP
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER	
YANG, CLARA I	

ART UNIT	PAPER NUMBER
2612	

DATE MAILED: 07/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/813,178	SENGUPTA ET AL.	
	Examiner	Art Unit	
	Clara Yang	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892) ✓
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. The examiner respectfully reminds the applicant to clearly indicate support for added or modified claim limitations in the remarks or arguments section of future amendments.

2. Applicant's arguments filed on 2 May 2006 with respect to claims 3, 5-14, 19-28, and 34-36 have been considered but are moot in view of the new ground(s) of rejection.

3. Applicant's arguments filed on 2 May 2006 have been fully considered but they are not persuasive.

a. Rejection of claims 1 and 29 under 35 USC §102(b) as being anticipated by Smith (US 2003/0025603)

In response to the applicant's statement on page 12 that the applicant "is unable to find any teaching within Smith where a determination is made of whether a user is within a predetermined distance of a wireless device," the examiner finds Smith teaching that limitation in Sections [0005], [0007], and [0011]. Smith's wireless device, which includes a personal digital assistant (PDA), determines that a valid master authenticator 10 is within a predetermined distance by transmitting a query to determine if a master authenticator 10 is present and "logged on" (see Section [0011], lines 20-24). Per Smith, master authenticator 10's transmitter 16 is authorized to transmit information only after a successful user login (see Section [0007], lines 28-31). Once transmitter 16 is authorized to transmit information, master authenticator 10 monitors the user's immediate surrounding area to determine whether a compatible electronic device (e.g., a PDA) capable of receiving master authenticator 10's information is present and transmits the information if the compatible PDA is present (see Section [0007], lines 34-38). The examiner understands that Smith's master authenticator 10 determines that a compatible PDA

is present when a query is received from the PDA, as described in Section [0011], lines 20-24 (also see Fig. 2, step 50), and that transmitter 16 then transmits information indicating successful authentication and user login in response to receiving the query (see Fig. 2, step 60). Smith's PDA then (1) receives master authenticator 10's information indicating that a user is logged on (i.e., authenticated) and (2) determines that master authenticator 10 is valid (i.e., is in the PDA's database) based on the received information (see Section [0011], lines 20-31). In other words, after receiving a signal from a master authenticator 10, Smith's PDA determines whether a valid master authenticator 10 is within a predetermined distance of the PDA, as called for in claims 1 and 29. Since the applicants omit specifying how the wireless device determines whether a user is within a predetermined distance of the wireless device, Smith does teach the method of "determining, after receiving said wireless signal, whether said user is within a predetermined distance of the wireless device," and the examiner maintains the previous rejection of claims 1 (and its dependent claim 2) and 29.

b. *Rejection of claim 15 under 35 USC §102(b) as being anticipated by Smith (US 2003/0025603) and rejection of claim 32 under 35 USC §103(a) as being unpatentable over Smith (US 2003/0025603) in view of Deng et al. (US 2003/0043078)*

The applicant argues on page 14 that the controller "first receives an indication that a user has been authenticated by a wireless body appliance worn by a user and then determines whether the authenticated user is within a predetermined distance of said wireless device" and that "Smith does not disclose or suggest making such a determination after an indication has been received that a user has been authenticated." The examiner respectfully disagrees. As shown in Fig. 2 and explained in the above paragraph concerning claim 1, Smith's authentication method comprises (a) a user wearing master authenticator 10 at step 22 and logging into master authenticator 10, wherein master authenticator 10 either denies or permits

the login at steps 26 and 30 respectively (see Section [0006]); (b) master authenticator 10's login means 14 authorizing transmitter 16 to transmit information at step 40 (see Section [0007], lines 28-31); (c) master authenticator 10 determining if a compatible PDA is in proximity at step 50 (see Section [0007], lines 34-37); (d) a personal digital assistant (PDA) transmitting a query to determine if master authenticator 10 is within a predetermined distance and logged on (see Section [0011, lines 20-24]); and (e) master authenticator 10 determining that a compatible PDA is in proximity upon receiving the query, and transmitter 16 transmitting information to the PDA in response to the query at step 60 (see Section [0007], lines 37-38). In order for master authenticator 10 to transmit information, the user must be logged on (i.e., authenticated) (see Sections [0006], [0007], and [0016]). Furthermore, Smith's PDA determines that an authenticated user is within a predetermined distance of 5-100 feet when the PDA (1) receives a response from master authenticator 10 and (2) determines that the master authenticator 10 is valid (i.e., is in the PDA's database). Consequently, Smith does teach a PDA controller that "first receives an indication that a user has been authenticated by a wireless body appliance worn by a user and then determines whether the authenticated user is within a predetermined distance of said wireless device." Since the applicants omit specifying how the wireless device determines whether a user is within a predetermined distance of the wireless device, the examiner maintains the previous rejection of claims 15 (and its dependent claims 16 and 18) and 32 (and its dependent claim 33).

c. *Rejection of claims 4 and 17 under 35 USC §103(a) as being unpatentable over Smith (US 2003/0025603) as applied to claims 1 and 15, and further in view of Overy et al. (US 2003/0220765)*

On page 17, the applicant argues that Overy fails to disclose or suggest a determination being made of whether a user is within a predetermined distance of a wireless device by

determining whether a power level being received from a wireless body appliance being worn by a user is above a threshold. The examiner respectfully disagrees. Overy teaches two Bluetooth™ wireless devices 21A and 21B, wherein device 21A is a wireless network server node (i.e., a wireless device) and device 21B is a PDA (i.e., a wireless body appliance) (see Section [0034]). Per Overy, device 21A's processor 26A estimates the distance to PDA 21B and determines whether or not to permit a connection to PDA 21B in conformity with a stored distance value that may be a security perimeter or a preprogrammed distance. If the distance indicates that PDA 21B is within the security perimeter, key exchange and subsequent secure communication is established (see Section [0034]). Though Overy discloses that the distance is determined by measuring the loop delay in this example, Overy teaches in Section [0045] that measuring received signal strength (i.e., power level) reduces distance measurement time. In other words, device 21A determines the distance to PDA 21B by measuring the received signal strength instead of measuring the loop delay in order to save time. Overy does fail to expressly teach that PDA 21B is within the security perimeter when device 21A determines that the received signal strength is above a threshold level, but one of ordinary skill in the art recognizes that a received signal strength must be compared to a threshold level representing the received signal strength for the outer boundary of the security perimeter in order to determine if PDA 21B is inside the security perimeter; thus Overy does teach a wireless device determining whether a power level being received from a wireless body appliance being worn by a user is above a threshold in order to determine whether a user is within a predetermined distance of a wireless device, and the examiner maintains the previous rejection of claims 4 and 17.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claim 3 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 3 has been amended to define "predetermine distance" of claim 1 as being "less than a wireless range of said wireless body appliance." The applicant's specification fails to support such limitation.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, 15, 16, 18, and 29 are rejected under 35 U.S.C. 102(b) as being anticipated by Smith (US 2003/0025603).

Referring to claims 1 and 29, Smith teaches a master authenticator 10 (i.e., a wireless body appliance) that is worn by a user and wirelessly transmits information associated with the

user to a remotely located electronic device (i.e., a wireless device), which includes a personal digital assistant (PDA) (see Abstract and Sections [0005]-[0007] and [0011]). As shown in Fig. 2, Smith's master authenticator 10 determines if it is worn by a user via sensor 12 at step 20 (see Section [0006]). If sensor 12 indicates that a user is properly wearing master authenticator 10 at step 22, master authenticator 10 allows the user to login and authenticates the user based on the login (see Sections [0006] and [0016]). Once a user successfully logs in, master authenticator 10's login means 14 authorizes transmitter 16 to transmit secure information (i.e., information associated with the user) at step 40 (see Section [0007]). Master authenticator 10 then monitors the immediate surrounding area to determine whether a compatible PDA (i.e., wireless device) is present at step 50 (see Section [0007]). Because Smith discloses that a PDA determines that a valid master authenticator 10 is within a predetermined distance by transmitting a query to determine if a master authenticator 10 is present and "logged on" (see Section [0011], lines 20-24), the examiner understands that Smith's master authenticator 10 determines that a compatible PDA is present at step 50 when a query is received from the PDA (as described in Section [0011], lines 20-24) and that transmitter 16 then transmits information indicating successful authentication and user login in response to receiving the query (see Fig. 2, step 60). As called for in claims 1 and 29, Smith's PDA then (a) receives master authenticator 10's wireless signal containing information that indicates that an authenticated user is logged on (see Sections [0007] and [0011]); (b) determines from the wireless signal that master authenticator 10 is valid (i.e., is in the PDA's database) based on the received information (see Section [0011], lines 20-31); and (c) automatically logs in the user if master authenticator 10 is a valid master authenticator (see Section [0011]). Smith's PDA determines that an authorized user is within a predetermined distance of the PDA when the PDA (1) receives master authenticator 10's

information indicating that an authenticated user and successful login and (2) determines that master authenticator 10 is in the PDA's database (see Section [0011]). In Section [0011], lines 20-24, Smith teaches that when powering on the PDA, the PDA's software application first sends out a query to determine if a valid master authenticator is present and "logged on." In other words, the process described in Section [0011], lines 20-31, begins while the PDA is initially powered off; thus the user is not logged in the PDA. Because Smith discloses that the PDA continues with a login routine that the user must complete before accessing the PDA when the PDA fails to find a valid master authenticator present and that the PDA continues "uninterrupted" when the PDA finds a valid master authenticator, the examiner understands that the PDA automatically logs in the user when the PDA finds a valid master authenticator.

Regarding claim 2, Smith teaches that master authenticator 10 comprises (a) at least one biometric sensor (see Sections [0006] and [0016]); (b) a biometric authentication unit that determines whether the user is authorized with master authenticator 10 based on the user's biometric information (see Sections [0005], [0006], [0008], and [0016]); and (c) transmitter 16 that transmits a wireless signal indicating that the user has been authenticated when the biometric authentication unit determines that the user is authorized (see Fig. 2, step 60 and Sections [0005], [0007], [0008], and [0016]).

Referring to claims 15 and 16, Smith discloses a wireless device that includes a PDA, such a Palm™ devices (see Section [0011]). Though Smith fails to expressly teach the details of the PDA, Palm™ devices all have: (a) at least a display and control buttons (i.e., a user interface), as called for in claims 15 and 16 and (b) a controller that controls the operation of the PDA, accepts input from a user via the control buttons, and delivers output to the user. In addition, Smith's PDA has (c) a Bluetooth™ transceiver to support wireless communication

with another PDA or master authenticator 10 (see Section [0011]); and (d) a controller having a software application that enables the PDA to receive an indication that the user has been authenticated by master authenticator 10, determine the authenticated user is within a predetermine distance by transmitting a query and receiving master authenticator 10's response to the PDA's query, and log in the authenticated user if master authenticator 10's response has been received (see Fig. 2, steps 50 and 52; and Sections [0005]-[0008], [0011], and [0016]). It is understood that the PDA automatically logs in an authorized user upon receiving master authenticator 10's secure information at step 52 of Fig. 2 because a user must manually login when the PDA fails to detect a valid master authenticator 10 (see Section [0011]).

Regarding claim 18, Smith teaches that the PDA is configured in accordance with a Bluetooth™ protocol (see Section [0011]).

8. Claims 7, 8, and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Prokoski et al. (US 6,850,147).

Referring to claim 7, Prokoski teaches a personal biometric key (PBK) 104, as shown in Fig. 1, comprising (a) biometric sensor 110 that measures biometric information from a user wearing the personal biometric key, which is a mobile telephone or a personal digital assistant (PDA) (see Col. 10, lines 15-22); (b) analyzer 120 (i.e., biometric authentication unit) that determines whether the user is an authorized user associated with PBK 104 based on the biometric information (see Col. 10, lines 20-28); and (c) Bluetooth™ transmitter 140 that transmits a user's personal code, which indicates that the user has been authenticated based on the user's biometric information (see Col. 10, lines 20-28). Per Prokoski, the preferred PBK 104 uses a dual-band visual and infrared camera for providing dual-band face recognition (see Col. 9, lines 30-60); thus Prokoski's biometric sensor 110 includes a camera.

Regarding claim 8, as explained in the previous rejection of claim 7, Prokoski's PBK 104 is a mobile telephone, which is wearable.

Regarding claim 11, as explained in the previous rejection of claim 7, Prokoski's PBK 104 includes Bluetooth™ transmitter 140, which is a wireless transmitter configured in accordance with a Bluetooth™ protocol.

9. Claims 7 and 8 are rejected under 35 U.S.C. 102(e) as being anticipated by Kotzin (US 2004/0257196).

Referring to claims 7 and 8, Kotzin teaches a wireless communication device 300 (i.e., wireless body appliance), as shown in Fig. 3 and called for in claim 7, comprising (a) microphone 206, fingerprint scanner bar 208, and embedded camera 210 that measure biometric information from a user wearing wireless communication device 300 (see Sections [0016], [0018], [0020], and [0034]); (b) controller 306 (i.e., a biometric authentication unit) that determines whether the user is an authorized user associated with wireless communication device 300 (see Sections [0024] and [0034]); and (c) wireless transmitter 304 that transmits a signal indicating that the user has been authenticated when controller 306 determines that the user is an authorized user (see Sections [0014]-[0016], [0022], and [0027]). Kotzin teaches that using camera 210 for hand, iris, and face recognition (see Section [0021]); thus Kotzin's camera 210 is a hand geometry sensor. Kotzin adds that a retina scanner, though less favored, is also available for wireless communication device 300 (see Section [0021]). Because Kotzin discloses that controller 306 enables the function of or provides access to wireless communication device 300 when a user is authorized using one of the biometric devices 206, 208, and 210, it is understood that telephone calls (i.e., signals) from wireless communication device 300 indicate that the user

has been authenticated. As called for in claim 8, Kotzin's wireless communication device 300 is a cellular telephone (see Section [0017]).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 3, 4, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) as applied to claims 1 and 15 above, and further in view of Overy et al. (US 2003/0220765).

Regarding claims 3, 4, and 17, though Smith teaches that master authenticator 10 (or the remotely located electronic device, such as a PDA or cellular telephone) is able to determine if the electronic device (or master authenticator 10) is within a predetermined distance of 5-100 feet (see Sections [0005], [0007], and [0011]), Smith fails to expressly teach that (1) the predetermines distance is less than a wireless range of master authenticator 10, as called for in

claim 3, and (2) master authenticator 10 is determined to be within the predetermined distance based on its received signal strength at the PDA, as called for in claims 4 and 17.

In an analogous art, Overy discloses a method for enhancing security in a wireless network using distance measurement techniques (see Abstract). Overy's method, as shown in Fig. 4, comprises (a) wireless transceiver 21A (i.e., wireless device) receiving a Bluetooth signal from wireless transceiver 21B (i.e., a wireless body appliance), such as a PDA, at step 33 (see Sections [0032]-[0034]); (b) transceiver 21A determining whether the PDA is within a predetermined distance at steps 33 and 34 (see Section [0045]); and (c) transceiver 21A automatically allowing secure communication with the PDA (i.e., the PDA to login) when the PDA is authorized via a successful key exchange and is within the predetermined distance at step 37 (see Sections [0037] and [0041]). As called for in claim 3, Overy teaches that the predetermined distance is less than the wireless range of the PDA and wireless transceiver 21A (see Figs. 1 and 2; and Sections [0026], [0027], and [0031]). In Fig. 4, Overy discloses that the distance is determined by measuring the loop delay. In Section [0045], however, Overy teaches that measuring received signal strength (i.e., power level) may be used to reduce the distance measurement time or further verify the measured distance, as called for in claims 4 and 17. In other words, device 21A determines the distance to a PDA (i.e., wireless transceiver 21B) by measuring the received signal strength instead of measuring the loop delay. In order for the PDA to be within a predetermined distance from transceiver 21A, the PDA's signal strength at transceiver 21A must exceed a threshold value representing the predetermined distance.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's method and electronic device as taught by Overy because (1) adding a device distance criterion to a Bluetooth™ network provides enhanced

security within a wireless network, and (2) using signal strength measurements to determine the device distance instead of loop delay reduces the distance measurement time (see Overy, Sections [0021] and [0045]).

13. Claims 5, 6, 19, 20, 30, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) as applied to claims 1 and 29 above, and further in view of Dorinski et al. (US 5,821,854).

Regarding claims 5, 6, 19, 20, 30, and 31, Smith omits teaching that the PDA's controller (a) automatically unlocks the PDA when the user is within a predetermined distance, the user is logged in, and the PDA is locked (as called for in claims 5, 19, and 30), or (b) automatically locks the PDA while keeping the user logged in when the user is not within a predetermined distance and the user is logged in (as called for in claims 6, 20, and 31).

In an analogous art, Dorinski teaches a security system 300, as shown in Fig. 3, comprising computer terminal 302 (i.e., a wireless device) that includes (a) antenna 322 (see Col. 3, lines 24-29 and 48-52); (b) a keyboard and monitor 306 (i.e., user interfaces) (see Col. 3, lines 35-39); (c) central processing unit (CPU) 304 (see Col. 3, lines 35-46); and (d) wireless receiver 312 coupled to antenna 322 to support wireless communication with portable radio 314 worn by user 316 (see Col. 3, lines 24-27 and 48-52). As called for in claims 5, 19, and 30, per Dorinski, CPU 304 is programmed to automatically unlock computer terminal 302 when (1) the user is within a predetermined distance of computer terminal 302 (see Col. 3, lines 39-46), (2) computer terminal 302 is active (i.e., the user is already logged on) (see Col. 2, lines 4-7 and Col. 3, lines 35-46), and (3) computer terminal 302 is locked (see Col. 3, lines 35-46). As called for in claims 6, 20, and 31, Dorinski's CPU 304 is further programmed to automatically lock computer terminal 302 when (1) the user is not within a predetermined distance of computer terminal 302 (see Col.

3, lines 29-39 and 52-56), and (2) computer terminal 302 is active (i.e., the user is already logged on) (see Col. 3, lines 32-46 and 48-56). Because Dorinski discloses that computer terminal 302 automatically returns to an active mode of operation without requiring user 316 to re-enter a password as soon as user 316 is within a predetermined distance of the computer terminal (see Col. 3, lines 43-46 and Col. 4, lines 14-20), it is understood that CPU 304 keeps user 316 logged in upon locking computer terminal 302. Dorinski adds that a locked computer terminal prevents anyone from operating the computer terminal (see Col. 2, lines 6-11 and Col. 3, lines 35-46) and an active (i.e., unlocked) computer terminal enables the authorized user (i.e., the party that is logged in) to access the computer and the data resident on the hard drive (see Col. 2, lines 4-6; Col. 3, lines 29-56; and Col. 4, lines 8-20).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's PDA as taught by Dorinski because a PDA controller that is programmed to (1) automatically unlock the PDA when the user is within a predetermined distance of the PDA, the user is logged in the PDA, and the PDA is locked (as called for in claims 5, 19, and 30) and (2) automatically lock the PDA while keeping the user logged in when the user is not within a predetermined distance of the PDA, the user is logged in the PDA, and the PDA is locked (as called for in claims 6, 20, and 31) provides a couple advantages, as explained by Dorinski: (1) a user does not have to actively lock the PDA after logging in if he/she intends to be step away from the PDA (see Col. 1, lines 26-30); and (2) a user does not have to re-enter a password once he/she returns to the PDA (see Col. 3, lines 43-46 and Col. 4, lines 14-20).

14. Claims 7, 8, 11, 12, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) in view of Prokoski et al. (US 6,850,147).

Referring to claims 7 and 8, Smith teaches all the limitations of claim 7, as explained in the previous 35 USC 102(b) rejection of claim 2, except that the biometric sensor includes a camera, as called for in the last limitation of claim 7. Smith also omits teaching that master authenticator 10 includes a mobile telephone (i.e., wearable telephone), as called for in claim 8.

In an analogous art, as explained in the previous 35 USC 102(e) rejection of claims 7 and 8, Prokoski teaches a personal biometric key (PBK) 104, as shown in Fig. 1, comprising biometric sensor 110 that measures biometric information from a user wearing PBK 104, which is a mobile telephone or a personal digital assistant (PDA) (see Col. 10, lines 15-22), as called for in claim 8. As called for in claim 7, Prokoski's preferred PBK 104 uses a dual-band visual and infrared camera for providing dual-band face recognition (see Col. 9, lines 30-60); thus Prokoski's biometric sensor 110 includes a camera.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's master authenticator 10 as taught by Prokoski because (1) a person generally carries his mobile telephone with him all day, thereby making the mobile telephone well-suited to be a master authenticator, and (2) a dual-band visual and infrared camera installed in the mobile telephone enables the mobile telephone to perform dual-band face recognition, which works for the entire human population and overcomes limitations of commonly-used biometric sensors (see Prokoski, Col. 1, lines 60-67 and Col. 2, lines 1-9).

Regarding claim 11, Smith teaches that master authenticator 10 is configured in accordance with a Bluetooth™ protocol (see Sections [0009], [0011], and [0014]).

Regarding claim 12, Smith's master authenticator 10 has a display or some other notification structure, such as an audible tone generator for generating a beep, that notifies the user that an event has occurred (see Sections [0011] and [0012]).

Regarding claim 14, though Smith and Prokoski are silent on master authenticator 10 having an illumination device as a notification structure, the examiner takes Official Notice that using an illumination device as a notification structure is well known. For example, pagers frequently have an illumination device that lights up when a page is received. In addition, a mobile telephone's display or keypad also lights up when a call is received. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith and Prokoski's method and system such that master authenticator 10 includes an illumination device as a notification structure because an illumination device is a more effective notification structure than an audible alert when the user is in a noisy environment.

15. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) in view of Prokoski et al. (US 6,850,147) as applied to claims 7 and 12 above, and further in view of Byrne (US 6,424,251).

Regarding claims 8 and 9, Smith and Prokoski omit teaching that master authenticator 10 is a hat (as called for in claim 8). Smith and Prokoski omit teaching that master authenticator 10 is a ring, a locket, a brooch, or a necklace (as called for in claim 9).

In an analogous art, Byrne teaches a personal electronic device notification system, as shown in Fig. 2. Per Byrne, personal electronic device 22 (i.e., a wireless device), such as portable telephones and PDAs, comprises transmitter 23 that transmits signal 26 (i.e., a wireless notification signal) to wristwatch 25 (i.e., a wireless body appliance) containing alert mechanism 24 (see Col. 1, lines 16-20; Col. 2, lines 55-65). The alert mechanism shown in Fig. 3 has notification structures including a vibration unit, an audible unit, an electrical stimulus unit, and a liquid crystal display (LCD) that displays information conveyed via signal 26 (see Col. 1, lines 59-64 and Col. 3, lines 11-29). Byrne's personal electronic device 22 (hereinafter referred to

as a "cellular phone") has (a) a user interface that enables a user to configure the cellular phone such that phone is set up to use an alert mechanism (see Col. 3, lines 30-35); thus the cellular phone must also have (b) a controller that controls the cellular phone based on the configuration entered by the user via a user interface and signals received from control mechanisms (see Col. 3, lines 30-45 and Col. 4, lines 12-53). Byrne's cellular phone also comprises (c) a transmitter and receiver to transmit wireless signals to an alert mechanism and to receive wireless signals from each control mechanism's transmitter 63 (see Col. 4, lines 42-53). Byrne teaches that events include receiving a telephone call within the cellular phone and that the user configures the phone such that it notifies the user of events (see Col. 3, lines 7-17 and 38-45). Byrne suggests incorporating alert mechanism 24 into any item, in addition to wrist watch 25, that is frequently worn by, near, or in contact with the body of a cellular phone's user (see Col. 2, lines 66-67 and Col. 3, lines 1-4). As called for in claims 8 and 9, this item, per Byrne, includes a hat or a piece of jewelry (see Col. 3, lines 2-5). Though Byrne omits specifying that the piece of jewelry be a ring, locket, a brooch, or a necklace, the examiner takes Official Notice that rings, lockets, brooches, and necklaces are all well known types of jewelry; thus it would been obvious to one having ordinary skill in the art at the time the invention was made to modify Byrne's wireless body appliance such that alert mechanism 24 is incorporated into a ring, locket, brooch, or a necklace since rings, lockets, brooches, and necklaces are pieces of jewelry worn by, near, or in contact with the body of a cellular phone's user.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith and Prokoski's method and system as taught by Byrne because incorporating master authenticator 10 into any item that is frequently worn by the user of the PDA, such as a hat, a ring, locket, brooch, or a necklace, eliminates the need for the user

to remember to carry master authenticator 10 in order to access the PDA, thereby making the system more user-friendly.

16. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kotzin (US 2004/0257196) as applied to claim 7 above, and further in view of Bianco et al. (US 6,256,737).

Regarding claim 10, though Kotzin's wireless communication device has 3 (i.e., N=3) biometric sensors (i.e., microphone 206, fingerprint scanner bar 208, and camera 210), Kotzin's controller 306 only requires a biometric match for 1 (i.e., M=1) of biometric sensors 206, 208, and 210 to determine that the user is an authorized user.

In an analogous art, Bianco teaches network system 202, as shown in Fig. 2, comprising a plurality of user computers 208, wherein each user computer 208 has one or more biometric devices attached to it such that a user is authenticated by biometric system 102 prior to access user computer 208 (see Col. 12, lines 12-23). Bianco's biometric devices include those that measure hand geometry, retina and facial images, breath (i.e., body chemistry), etc. (see Col. 12, lines 54-57). Bianco discloses that biometric system 102 is governed by biometric policies 504, such as an OR biometric policy, which would only require a user to pass either one of at least two biometric devices, or an AND biometric policy, which would require a user to be tested on at least two biometric devices and pass all the biometric devices that he/she was tested on (see Col. 30, lines 55-67 and Col. 31, lines 1-7). Fig. 18 illustrates the AND policy. Per Bianco, n number of biometric devices (where n is at least 2) is determined from a list of biometric devices at step 1802. Assuming that a user is to be tested on 2 (M=2) of the biometric devices using the AND policy, Bianco's biometric system 102 requires the user to pass both biometric devices at steps 1808 and 1814 (see Col. 32, lines 65-67 and Col. 33, lines 1-26). Because Bianco teaches that a user can be tested on more than 2 biometric devices (see Col. 33, lines 26-53); thus the list of

biometric devices includes at least 3 biometric devices (i.e., N≥3). Consequently, Bianco does teach biometric system 102 requiring a biometric data match for at least two (i.e., M=2) of the at least 3 (i.e., N=3) biometric devices to determine that a user is authorized.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Kotzin's system and method as taught by Bianco because the combination of two or more biometric devices for authenticating a user enables the user to adjust the level of security protecting master authenticator 10 and the associated wireless device as needed (see Bianco, Col. 30, lines 4-14).

17. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) in view of Prokoski et al. (US 6,850,147) as applied to claim 12 above, and further in view of Chadha (US 2004/0176107).

Regarding claim 13, Smith's master authenticator 10, as modified by Prokoski, includes a Bluetooth™ receiver that receives a wireless notification signal from a PDA or a cellular telephone (i.e., wireless devices), wherein the wireless notification signal identifies that an event has occurred (see Smith, Sections [0011] and [0012]). Though Smith and Prokoski's master authenticator 10 has a plurality of notification structures (e.g., a display and an audible alert, as described in Sections [0011] and [0012]), Smith and Prokoski are silent on the wireless notification signal identifying the type of notification structure that is to be used to notify the user of the event.

In an analogous art, Chadha teaches wireless device 200 (hereinafter referred to as "wireless body appliance 200"), such as a cellular phone (i.e., a wearable telephone) or a PDA (see Section [0013]). Chadha's wireless body appliance 200 includes a plurality of notification structures that notifies a user that an event has occurred: a visual notification structure that

displays messages or video, an audio notification structure, and a notification structure that indicates an event by initiating a user-specified action on wireless body appliance 200 (see Sections [0019] and [0030]). As called for in claim 13, Chadha's wireless body appliance 200 also has a wireless receiver that receives reminders (i.e., wireless notification signals) from a wireless service provider's equipment, wherein the wireless notification signal identifies an event that has occurred (e.g., a user is in a user-specified location for performing a task) and identifies the type of notification structure to be used to notify the user of the event (see Sections [0014], [0015], [0019], [0020], [0027], and [0030]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith and Prokoski's wireless notification signal as taught by Chadha because a wireless notification signal that includes information identifying a type of notification to be used by wireless body appliance 200 to notify the user of an event enables a user to select an appropriate notification for each event, thereby making the system flexible and user-friendly.

18. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) as applied to claim 15 above, and further in view of Chadha (US 2004/0176107).

Regarding claim 21, as explained in the previous rejection of claim 13, the controller of Smith's wireless device is programmed to send a wireless notification signal to master authenticator 10 when a predetermined event occurs (see Sections [0011] and [0012]). Though Smith's master authenticator 10 has a plurality of notification structures (e.g., a display and an audible alert) as described in Sections [0011] and [0012], Smith is silent on the wireless device's controller sending a wireless notification signal that identifies the type of notification structure that is to be used to notify the user of the event.

In an analogous art, Chadha teaches that a wireless service provider's equipment transmitting a wireless notification signal to wireless device 200, wherein the wireless notification signal is a text message (e.g., "Remind me to buy item X whenever I pass near store Y" or "Remind me to drop off item W whenever I pass location Z"), an audio prompt, a video prompt, or an initiation of a user-defined action on the wireless device, etc. (see Sections [0019] and [0030]); thus Chadha's wireless notification message identifies the type of notification structure to be used to notify the user of a predetermined event and causes wireless device 200 to notify the user of the event.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's wireless device and wireless notification signal as taught by Chadha because Smith teaches a controller that uses a wireless transmitter to transmit a wireless notification signal to a wireless receiver whereas Chadha teaches a controller that uses a wireless transmitter to transmit a wireless notification signal to a wireless receiver, wherein the wireless notification signal identifies the type of notification structure that is to be used by the wireless receiver to notify the user of the event, thereby making the system flexible and user-friendly by enabling a user to select an appropriate notification for each event.

19. Claims 22-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) in view of Chadha (US 2004/0176107).

Referring to claim 22, Smith teaches that a PDA or cellular telephone (a) identifies an event for which a user is to be notified via master authenticator 10 and (b) transmits a wireless notification signal to master authenticator 10, causing master authenticator 10 to notify the user of the occurrence (see Sections [0011] and [0012]). Such events include an incoming phone call when the wireless device is a cellular telephone (see Section [0012]) and the receipt of a request

from a second party's PDA when the wireless device is a PDA (see Section [0011]). Smith fails to specify that the request received from a second party's PDA is an email or instant message or that the cellular telephone transmits a wireless notification signal to master authenticator 10 when it receives an email or instant message.

In an analogous art, Chadha teaches a method and wireless network system comprising (a) identifying one or more events from which a user is to be notified via wireless device 200 (hereinafter referred to as "wireless body appliance 200"), such as a cellular phone or a PDA (see Sections [0014], [0017], and [0021]), and (b) transmitting a wireless notification signal to wireless body appliance 200 to notify the user when an identified event occurs (see Sections [0014], [0015], [0017], and [0021]). Chadha's events include a scheduled task reminder occurring (see Sections [0014], [0017], and [0021]). Chadha also teaches that wireless body appliance 200 receives emails or instant messages (see Section [0019]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to Smith's method as taught by Chadha because a wireless device that transmits a wireless notification signal to master authenticator 10 when the wireless device receives an email or instant message in addition to a phone call enables a user to determine the receipt of an email or instant message without having to check the wireless device itself, thereby reducing the likelihood of the user missing the receipt of an email or instant message in addition to phone calls when the wireless device is in a pocket, purse, briefcase, etc.

Regarding claims 23-26, Smith omits disclosing that (1) the wireless notification signal includes information identifying one or more types of notification to be used by master authenticator 10 to notify the user of an event occurrence (as called for in claim 23); (2) a user selects an event from a plurality of available events (as called for in claim 24); (3) the step of

identifying types of notification to be given by the PDA in different types of locations (as called for in claim 25); and (4) the steps of determining a present location of the wireless device, determining whether one or more types of notification have been identified for the present location, and configuring the wireless notification signal to provide the identified types of notification within the wireless body appliance when one or more types of notification have been identified from the present location (as called for in claim 26).

Chadha's method includes the step of a wireless service provider's network equipment transmitting a wireless notification signal to wireless body appliance 200, wherein the wireless notification signal is a prompt, an email, instant message, an initiation of a user-defined action on the wireless device, etc. (see Sections [0019] and [0030]). Chadha teaches that a prompt includes audio, video, and/or text data and that the wireless service provider causes Task Management Client Application 210 to remotely initiate actions on the wires device (see Sections [0019] and [0030]). Because Chadha's wireless notification signal is an audio prompt, video prompt, an email, an instant message, an initiation of a user-defined action on the wireless device, etc., the wireless notification signal must include information identifying a type of notification to be used by wireless body appliance 200 to notify the user of an event, as called for in claim 23. As called for in claim 24, Chadha's method further includes a user selecting one or more events from a plurality of available events. For example, exemplary reminder (i.e., event) entries in a task reminder database include "Remind me to buy item X whenever I pass near store Y" or "Remind me to drop off item W whenever I pass location Z" (see Section [0014]). Another type of event includes configuring a child's wireless body appliance 200 to generate and send an event trigger signal to a parent's wireless body appliance 200 reminding the parent to call the child when the child is leaving a predefined radius of a school or home

zone (see Sections [0021] and [0033]). A further type of event includes a one-time event or a recurring event (see Section [0022]). And as called for in claim 25, Chadha's method comprises the step of identifying the appropriate type of notification (e.g., "Remind me to buy item X whenever I pass near store Y" or "Remind me to drop off item W whenever I pass location Z") to be given by wireless body appliance 200 based on wireless body appliance 200's current location (see Sections [0014], [0015], [0017]-[0020], and [0027]). Finally, as called for in claim 26, Chadha's method includes the steps of (a) determining the present location of wireless body appliance 200 (see Fig. 3 and Sections [0014]-[0018] and [0034]); (b) determining whether a notification has been identified for the present location (see Sections [0014], [0015], [0017], [0018], and [0027]); and (c) configuring a wireless notification signal to provide the identified type of notification within wireless body appliance 200 when an event has been identified for the present location (see Sections [0014]-[0116], [0019]-[0021], [0027], and [0030]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's method as taught by Chadha because (1) wireless notification signal that includes information identifying a type of notification to be used by wireless body appliance 200 to notify the user of an event (as called for in claim 23) enable a user to select an appropriate notification for each event, thereby making the system flexible and user-friendly; (2) a plurality of available events, such as location-based task reminders, from which a user selects one or more event (as called for in claim 24) enhances the functionality of master authenticator 10 (see Chadha, Sections [0003]-[0005]); (3) the method of identifying the appropriate type of notification (e.g., "Remind me to buy item X whenever I pass near store Y" or "Remind me to drop off item W whenever I pass location Z") to be given by master authenticator 10 based on master authenticator 10's current location (as called for in claim 25)

enables master authenticator 10 to remind a user of a task based on the user's location, thereby providing the user with the sophisticated functionality of location-based task reminders (see Chadha, Sections [0003]-[0005]); and (4) the method of determining the present location of Smith's wireless device (e.g., a cellular telephone or PDA), determining whether a type of notification has been identified for the wireless device's present location, and configuring a wireless notification signal to provide a specific notification within master authenticator 10 when an event has been identified for the present location (as called for in claim 26) provides the user with the sophisticated functionality of location-based task reminders (see Chadha, Sections [0003]-[0005]) and the convenience of receiving event notifications at master authenticator 10 (see Smith, Sections [0011] and [0012]) without having to check the wireless device itself, thereby reducing the likelihood of the user missing the receipt of an email or instant message in addition to phone calls when the wireless device is in a pocket, purse, briefcase, etc.

Regarding claim 27, though Smith is silent on master authenticator 10 having an illumination device as a notification structure, the examiner takes Official Notice that using an illumination device as a notification structure is well known. For example, pagers frequently have an illumination device that lights up when a page is received. In addition, a mobile telephone's display or keypad also lights up when a call is received. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's method and system such that master authenticator 10 includes an illumination device as a notification structure because an illumination device is a more effective notification structure than an audible alert when the user is in a noisy environment.

Regarding claim 28, Smith teaches that master authenticator 10 is a piece of jewelry, such as a bracelet or a wristwatch (see Sections [0006] and [0008]).

20. Claims 32 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) in view of Deng et al. (US 2003/0043078).

Referring to claim 32, Smith, as explained in the previous rejection of claim 15, teaches all the limitations but omits teaching that the PDA, which must have at least an antenna for communicating via a Bluetooth™ protocol (see Section [0011]), has at least one dipole antenna.

In an analogous art, Deng teaches a dipole antenna module formed on a printed circuit board of a Bluetooth™ chip for devices such as PDAs and mobile phones (see Sections [0005] and [0031]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's PDA as taught by Deng because forming a dipole antenna on a printed circuit board saves space on the printed circuit board and enables the main function circuit and the dipole antenna to be integrated on a single chip for miniaturization (see Deng, Sections [0006], [0013] and [0015]).

Regarding claim 33, Smith teaches that the PDA is configured in accordance with a Bluetooth™ protocol (see Section [0011]).

21. Claims 34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) in view of Deng et al. (US 2003/0043078) as applied to claim 32 above, and further in view of Dorinski et al. (US 5,821,854).

Regarding claims 34 and 35, Smith and Deng are silent on the PDA's controller being programmed to (1) automatically unlock the PDA when the user is within a predetermined distance of the PDA, the user is logged in the PDA, and the PDA is locked (as called for in claim

34) or (2) automatically lock the PDA while keeping the user logged in when the user is not within a predetermined distance of the PDA, the user is logged in the PDA, and the PDA is locked (as called for in claim 35).

In an analogous art, as explained in the previous rejection of claims 5, 6, 30, and 31, Dorinski's CPU 304, as called for in claim 34, is programmed to automatically unlock computer terminal 302 when (1) the user is within a predetermined distance of computer terminal 302 (see Col. 3, lines 39-46), (2) computer terminal 302 is active (i.e., the user is already logged on) (see Col. 2, lines 4-7 and Col. 3, lines 35-46), and (3) computer terminal 302 is locked (see Col. 3, lines 35-46). As called for in claim 35, Dorinski's CPU 304 is further programmed to automatically lock computer terminal 302 when (1) the user is not within a predetermined distance of computer terminal 302 (see Col. 3, lines 29-39 and 52-56), and (2) computer terminal 302 is active (i.e., the user is already logged on) (see Col. 3, lines 32-46 and 48-56). Because Dorinski discloses that computer terminal 302 automatically returns to an active mode of operation without requiring user 316 to re-enter a password as soon as user 316 is within a predetermined distance of the computer terminal (see Col. 3, lines 43-46 and Col. 4, lines 14-20), it is understood that CPU 304 keeps user 316 logged in upon locking computer terminal 302.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith and Deng's PDA as taught by Dorinski because a PDA controller that is programmed to (1) automatically unlock the PDA when the user is within a predetermined distance of the PDA, the user is logged in the PDA, and the PDA is locked (as called for in claim 34) and (2) automatically lock the PDA while keeping the user logged in when the user is not within a predetermined distance of the PDA, the user is logged in the PDA, and the PDA is locked (as called for in claim 35) provides a couple advantages, as explained by

Dorinski: (1) a user does not have to actively lock the PDA after logging in if he/she intends to be step away from the PDA (see Col. 1, lines 26-30); and (2) a user does not have to re-enter a password once he/she returns to the PDA (see Col. 3, lines 43-46 and Col. 4, lines 14-20).

22. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Smith (US 2003/0025603) in view of Deng et al. (US 2003/0043078) as applied to claim 32 above, and further in view of Chadha (US 2004/0176107).

Regarding claim 36, as explained in the previous rejection of claim 21, the controller of Smith's wireless device, as modified by Deng, is programmed to send a wireless notification signal to master authenticator 10 when a predetermined event occurs (see Smith, Sections [0011] and [0012]). Though Smith and Deng's master authenticator 10 has a plurality of notification structures (e.g., a display and an audible alert) (see Smith, Sections [0011] and [0012]), Smith and Deng are silent on the wireless device's controller sending a wireless notification signal that identifies the type of notification structure that is to be used to notify the user of the event.

In an analogous art, Chadha teaches that a wireless service provider's equipment transmitting a wireless notification signal to wireless device 200, wherein the wireless notification signal is a text message (e.g., "Remind me to buy item X whenever I pass near store Y" or "Remind me to drop off item W whenever I pass location Z"), an audio prompt, a video prompt, or an initiation of a user-defined action on the wireless device, etc. (see Sections [0019] and [0030]); thus Chadha's wireless notification message identifies the type of notification structure to be used to notify the user of a predetermined event and causes wireless device 200 to notify the user of the event.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Smith's wireless device and wireless notification signal as

taught by Chadha because Smith teaches a controller that uses a wireless transmitter to transmit a wireless notification signal to a wireless receiver whereas Chadha teaches a controller that uses a wireless transmitter to transmit a wireless notification signal to a wireless receiver, wherein the wireless notification signal identifies the type of notification structure that is to be used by the wireless receiver to notify the user of the event, thereby making the system flexible and user-friendly by enabling a user to select an appropriate notification for each event.

Conclusion

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

⌘⌘⌘

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clara Yang whose telephone number is (571) 272-3062. The examiner can normally be reached on 9:00 AM - 7:30 PM, Monday - Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wendy Garber can be reached on (571) 272-7308. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CY
12 July 2006

BRIAN ZIMMERMAN
PRIMARY EXAMINER